

"Method of executing a cryptographic protocol between
two electronic entities"

ABSTRACT

Perfected cryptographic protocol making it possible to counter attacks based on the analysis of the current consumption during the execution of a DES or similar.

According to the invention, a message (M) is processed by two entities (A
and B) and the entity (B) subject to attack executes a chain of operations known
as DES in which it is chosen to carry out a given operation ($O_1, O_2, O_3 \dots O_n$)
or the same operation complemented ($\bar{O}_1, \bar{O}_2, \bar{O}_3 \dots \bar{O}_n$), the choice being
random.

Figure 2